User Manual

iStorage®
SECURING THE MAINSTREAM

diskG®

formerly known as diskGenie

diskG®

iStorage®
SECURING THE MAINSTREAM

Copyright © iStorage, Inc 2009. All rights reserved.

Windows is a registered trademark of Microsoft Corporation.
All other trademarks and copyrights referred to are the property of their respective owners.

Distribution of modified versions of this document is prohibited without the explicit permission of the copyright holder.

Distribution of the work or derivative work in any standard (paper) book form for commercial purposes is prohibited unless prior permission is obtained from the copyright holder.

DOCUMENTATION IS PROVIDED AS IS AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID

FC CE RoHS

All trademarks and brand names are the property of their respective owners.

Table of Contents

Introduction 4
Box contents 4
1. diskG Layout 5
2. Connecting the diskG 6
3. Connecting the diskG with USB Y-Cable 7
4. How do I use the diskG the first time? 7
5. What if I forget the User Password? 7
6. Entering the Standby Mode 8
7. Entering the User Mode 8
8. Exiting the User Mode 8
9. Entering the Admin Mode 9
10. Exiting the Admin Mode 9
11. Changing the Admin Password 10
12. Adding a new User Password 11
13. Deleting the User Passwords 11
14. Changing the User Password 11
15. Brute Force Protection 12
16. Completely resetting the diskG 13
17. Initializing and formatting the diskG after a complete reset 13
18. Hibernating, Suspending, or Logging off 15
19. Troubleshooting 16
20. Technical Support 20
21. Warranty and RMA information 20

diskG®

iStorage®
SECURING THE MAINSTREAM

Introduction

Looking for an effortless way to secure your data?

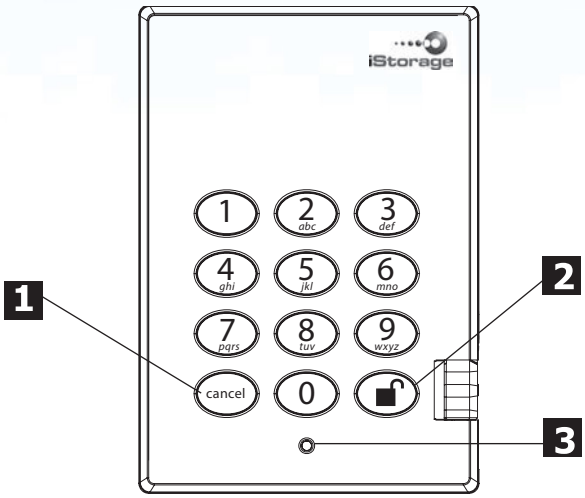
The iStorage diskG Secure Drive is the ultimate portable hard drive and secure storage system. With an easy-to use keypad design and software free setup, the diskG enables you to securely access the drive with your own unique PIN. Featuring your choice of 128-bit or 256-bit hardware encryption and USB 2.0 connection, the diskG provides seamless real-time encryption, keeping your data safe even if the hard drive is removed from its enclosure.

Box Contents

- iStorage diskG drive with integrated USB cable
- Travel Pouch
- USB Y-cable
- Quick Start Guide

1. diskG Layout

1. **Cancel** button
2. button
3. LED Indicator lights



The "**Cancel**" button can be used to:

- Cancel current operation
- Return to the previous step when you knowingly entered a wrong password
- Exit the Admin Mode

The button can be used to access the diskG and it can also be used as an OK acknowledgement in the following operations:

- Entering a password
- Confirming a new password

The LED indicator light displays the following colors to indicate the various modes of operation:

- RED: Standby Mode
- BLUE: Admin Mode
- GREEN: User Mode

The LED indicator light has other display methods to indicate different status of the diskG. Details are provided later in this chapter.

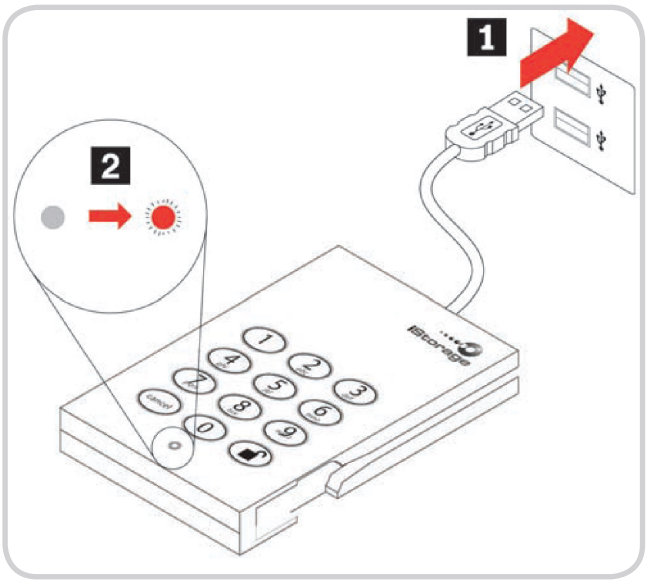
Be sure to review the following information before you begin to use the diskG.

Attention: Use only the included cables with your diskG. You might damage the drive if you use a cable not included with the diskG.

2. Connecting the diskG

1. Attach the integrated USB cable of the diskG drive to an available USB port on your computer, as shown below.

2. The diskG LED indicator light should glow **RED**.



Note: If the LED Indicator light does not power, use the included USB Y-cable Refer to directions on the following page

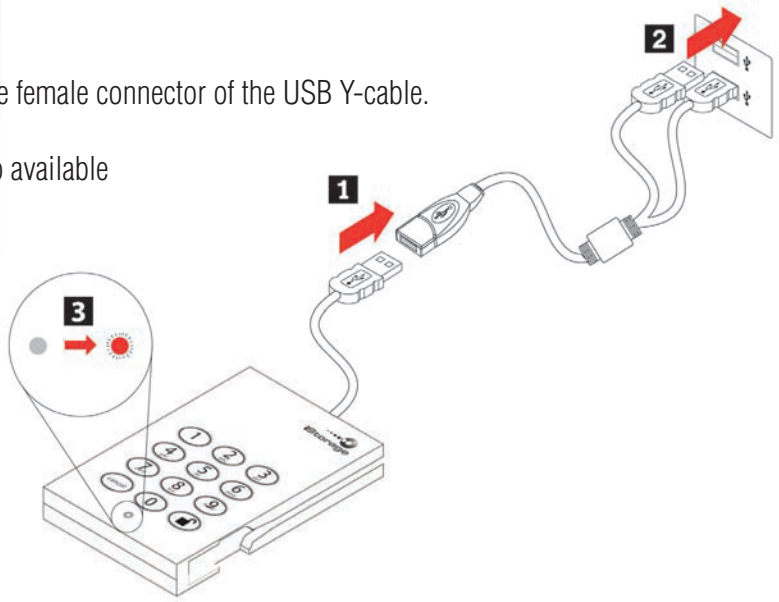
3. Connecting the diskG with USB Y-cable

If the LED indicator light does not power on a single USB connection, use the included USB Y-cable.

1. Attach the diskG's integrated USB cable to the female connector of the USB Y-cable.

2. Connect the two male USB connectors to two available USB ports on your computer.

3. The diskG LED indicator light should glow **RED**.



4. How do I use the diskG the first time?

You can use it in one of the following ways:

- Enter the Admin Mode with **123456** (default administrator password), and then you are able to change the Admin Password or create a User Password.

- Directly enter the Secure User Mode with **123456** (default Admin Password) to use the diskG.

5. What if I forget the User Password?

Use your Admin Password to enter Admin Mode, and then create another User Password in Admin Mode.

Caution: If you forget or lose your ADMIN password there is no way to access the drive. Even an IStorage employee will be unable to help you access your data. In the event that this happens, the only way to use the drive is to do a complete reset, which will reset the encryption key making all data on the drive unrecoverable and restore the to the default Admin Password **123456**.

See the Chapter "Completely Resetting the diskG" for instructions.

6. Entering the Standby Mode

The Standby Mode is the default mode of the diskG and is the gateway to other working modes.

To enter the Standby Mode, attach the diskG to your computer. The drive automatically goes into Standby Mode and the LED indicator light turns **RED**. In this mode, the diskG is locked. It cannot be recognized by **My Computer** and it does not provide either the regular functions or the encryption function. However, it enables you to enter and switch between the Admin Mode and the User Mode.

Attention: To switch between the Admin Mode and the User Mode, you are required to switch to the Standby Mode first, and then you can enter the mode of your choice.

7. Entering the User Mode

To enter the User Mode, do the following:

1. Attach the diskG to your computer. It enters the Standby Mode.

2. Enter the User Password or the Admin Password (the default Admin Password is **123456**) and press . The LED indicator light turns **GREEN** indicating that the drive is in the User Mode. If the LED indicator light flashes **RED**, you need to re-enter the correct password.

8. Exiting the User Mode

To exit the User Mode, double-click the **Safely Remove Hardware** icon from the Microsoft® Windows® desktop, and then remove the diskG from your computer.

Attach the diskG to your computer again and the LED indicator light turns **RED**. This indicates that you are in the Standby Mode.

9. Entering the Admin Mode

Note: The diskG cannot be recognized by the operating system in the Admin Mode.

To enter the Admin Mode, do the following:

1. Attach the USB cable to an available USB port on your computer. The diskG goes into the Standby Mode, and the LED indicator light turns **RED**.

2. Press and hold + 0 for five seconds until the LED indicator light flashes **RED**. This indicates that you can enter the Admin Password.

3. Enter the Admin Password and press . The default Admin Password is **123456**. The Secure Hard Drive is in Admin Mode when the LED indicator light has changed to **BLUE**.

Note: If the LED indicator light flashes **RED** for a few seconds, indicating the diskG has returned to the Standby Mode, go back to Step 2. This is due to one of the following conditions:

- You entered an incorrect Admin Password in Step 3.
- No activity was detected within two minutes in the Admin Mode.

10. Exiting the Admin Mode

To exit the Admin Mode, press the "**Cancel**" button in the Admin Mode until the LED indicator light turns **RED**. This indicates that you are in the Standby Mode.

11. Changing the Admin Password

This section provides information about managing your password in the Admin Mode.

You can change the Admin Password by doing the following:

1. Enter Admin Mode (refer to page 9 for details).
2. Press and hold + 9 until the LED indicator light flashes **BLUE**.
3. Enter the new password and press (The Password must be a minimum of 6 digits and a maximum of 16 digits). The LED indicator light flashes **GREEN** three times. See note below.
4. Re-enter the new Admin Password and press . The LED indicator light stays solid **GREEN** for two seconds and then solid **BLUE** indicating that the Admin Password has been changed successfully.

Note: If the LED indicator light flashes **RED** three times, this indicates that the password is less than 6 digits or more than 16 digits. Enter a password that contains 6 – 16 digits after the LED indicator light flashes **BLUE** intermittently.

1. If the LED indicator light flashes **RED** intermittently and then **BLUE** intermittently, go back to step 3. This is due to one of the following conditions:

- You waited longer than 10 seconds before entering a password.
- The new password was entered incorrectly.

2. If no activity is detected within two minutes in the Admin Mode, the diskG will return to the Standby Mode.

12. Adding a new User Password

You can add a new User Password by doing the following:

1. Enter the Admin Mode (refer to page 9 for details).
2. Press and hold + 1 until the LED indicator light flashes **BLUE** intermittently.
3. Enter a User Password and press (a minimum of 6 digits and a maximum of 16 digits). The LED indicator light will flash **GREEN** three times.
4. Re-enter the new User Password and press . If the LED indicator light stays solid **GREEN** for two seconds and then solid **BLUE**, the User Password was added successfully.

13. Deleting the User Passwords

You can delete all User Passwords by doing the following:

1. Enter the Admin Mode (refer to page 9 for details).
2. Press and hold 7 + 8 + for five seconds until the LED indicator light flashes **BLUE** intermittently. After the LED indicator light will flash **GREEN** three times and then **BLUE** intermittently.
3. Press and hold 7 + 8 + a second time for five seconds until the LED indicator light goes on solid **GREEN** for two seconds and then back to solid **BLUE**, this indicates that the User Passwords were deleted successfully.

14. Changing the User Password

You can change the User Password by doing the following:

1. Enter User Mode (refer to page 8 for details).
2. Press and hold + 1 until the LED indicator light flashes **RED**.
3. Enter your old password and press . The LED indicator light will turn **GREEN**, then change to flashing **BLUE**.
4. Enter the new password and press (The Password must be a minimum of 6 digits and a maximum of 16 digits). The LED indicator light will flash **GREEN** three times.
5. Immediately re-enter the new User Password and press . The LED indicator light will stay solid **GREEN** indicating that the User Password has been changed successfully.

15. Brute Force Protection

What is a Brute Force Attack?

A brute force attack is a method of defeating a cryptographic scheme by systematically trying a large number of possibilities; for example, a large number of the possible keys in a key space in order to decrypt a message.

In most schemes, the theoretical possibility of a brute force attack is recognized, but it is set up in such a way that it would be computationally infeasible to carry out. Accordingly, one definition of "breaking" a cryptographic scheme is to find a method faster than a brute force attack.

How does the diskG protect against brute force attack?

1. With the drive locked and in the standby state the LED indicator light will be solid **RED**.

2. After six tries to enter the correct user or admin password the keypad will not respond and LED indicator light will turn off. The drive will need to be unplugged from the USB port and replugged. This will be repeated for each six unsuccessful attempts.

3. If the user unsuccessfully tries to unlock the drive on his 50th try the keypad will lock and the LED indicator light will begin blinking quickly. Even after unplugging and replugging in the unit, the drive will remain locked and the LED indicator light will continue to blink rapidly.

4. Here are the steps to allow the user to unlock the keypad for 50 more attempts to unlock the drive.

    a. Unplug the device from the computer.

    b. Push and hold the number five key and plug-in the drive.

    c. The LED indicator light will be blinking, alternating **RED** and **GREEN** rapidly.

    d. Enter the code **5278879.**

    e. The keypad will unlock and will be in the standby state with the LED indicator light solid **RED**, this will allow only 50 more attempts.

    f. After a total of 100 attempts the drive will remain locked with the LED indicator light flashing **RED** quickly. You must now go through the reset process and reformat the drive to be able to use the drive again (see page 13 - Completely resetting the diskG).

16. Completely resetting the diskG

If you forget all the User Passwords or Admin Passwords, you can perform a complete reset to remove all the User Passwords, and restore the Admin Password to the default **123456**.

Attention: Completely resetting the diskG will reset the encryption key, in effect making all the data on the drive unrecoverable. You will need to partition and format the diskG with disk management applications. To perform a complete reset of the drive, do the following:

1. Press and hold the "**Cancel**" button while you attach the diskG to an available USB port on your computer. The LED indicator light will flash **BLUE** and **RED** alternately.

Note: If no activity is detected for 30 seconds in this step, the diskG will go into the Standby Mode.

2. Press and hold "**Cancel**" + 🔓 + **2** for 10 seconds until the LED indicator light flashes **RED** and **BLUE** intermittently, and then stops on a solid color. The LED indicator light will then turn solid **GREEN** for two seconds, followed by solid **RED**. You have successfully reset the diskG.

17. Initializing and formatting the diskG after a complete reset

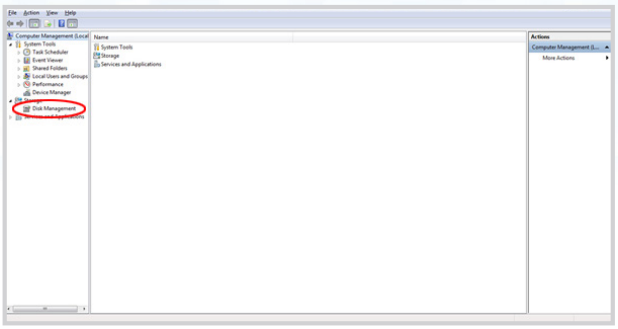
A complete reset of the diskG will erase all information and partition settings. You will need to initialize and format the diskG.

To initialize your diskG, do the following:

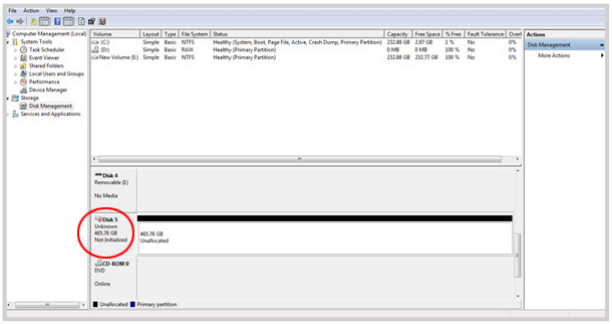
1. After a complete reset, attach the diskG to the computer.
2. Wait 5 seconds for the computer to recognize the device.
3. Enter the default User Password **123456** and press 🔓 to enter the User Mode.
4. Right-click **My Computer**, and then click **Manage** from the Windows desktop.

5. In the Computer Manage window, click **Disk Management**. In the Disk Management window, the diskG is recognized as an unknown device that is uninitialized and unallocated.

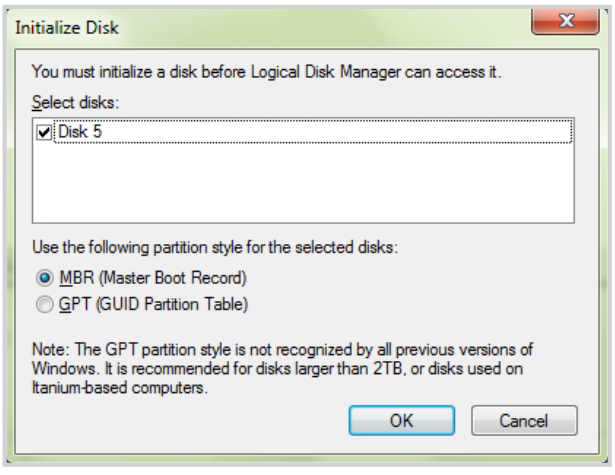
Note: If the Initialize Disk Wizard window opens, click **Cancel.**



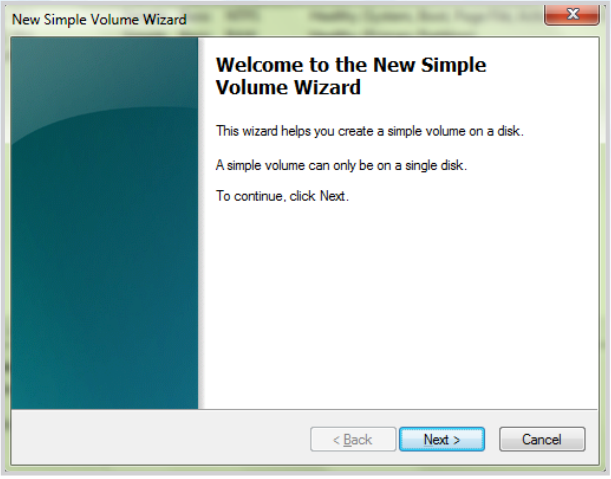
6. Right-click Unknown Disk, and then select Initialize Disk.



7. In the Initialize Disk window, click **OK**.


Initialize Disk
You must initialize a disk before Logical Disk Manager can access it.
Select disks:
Disk 5
Use the following partition style for the selected disks:
MBR (Master Boot Record)
GPT (GUID Partition Table)
Note: The GPT partition style is not recognized by all previous versions of Windows. It is recommended for disks larger than 2TB, or disks used on Itanium-based computers.
OK
Cancel

8. Right-click in the blank area under the Unallocated section, and then select New Simple Volume. The Welcome to the New Simple Volume Wizard window opens.


New Simple Volume Wizard
Welcome to the New Simple Volume Wizard
This wizard helps you create a simple volume on a disk.
A simple volume can only be on a single disk.
To continue, click Next.
< Back
Next >
Cancel

9. Click **Next**.

10. If you need only one partition, accept the default partition size and click **Next**.

11. Assign a drive letter or path and click **Next**.

12. Create a volume label, select Perform a quick format, and then click **Next**.

13. Click **Finish**.

14. Wait until the format process is complete. The diskG will be recognized and it is available for use.

18. Hibernating, Suspending, or Logging off from the Operating System

Be sure to save and close all the files on your diskG before hibernating, suspending, or logging off from the Windows operating system.

It is recommended that you log off the diskG manually before hibernating, suspending, or logging off from your system.

To log off the diskG, double-click Safely Remove Hardware on the Windows desktop and remove the diskG from your computer.

Attention: To ensure the data integrity of your diskG, be sure to lock or log off your diskG if you are:
- away from your computer
- using the switching user function by sharing a computer with others

19. Troubleshooting

This section contains troubleshooting information for the diskG. If you encounter any of the following problems when using the diskG, refer to the corresponding answers.

Q: How do I use the diskG the first time?

A: You can use it in one of the following ways:

- Enter the Admin Mode with **123456** (default administrator password), and then you are able to change the Admin Password or create a User Password.
- Directly enter the Secure User Mode with **123456** (default Admin Password) to use the diskG.

Q: What can I do if I forget the User Password?

A: Use your Admin Password to enter Admin Mode, and then create another User Password in Admin Mode.

Q: What can I do if I forget the Admin Password?

A: There is no other way to retrieve the Admin Password except a complete reset of the diskG. After a complete reset, all data will be lost and you will need to initialize, allocate and format the diskG manually. Then you will be able to use the default Admin Password **123456**.

Q: Why did the operating system not recognize the diskG after I enter the User Mode and completely reset the computer?

A: You need to initialize, allocate and format the diskG manually. For more information, refer to Initializing and formatting the Hard Drive after a complete reset in this manual.

Q: How do I use the diskG without a password?

A: As a full disk encryption product, the diskG can never be used without a password.

Q: What encryption algorithm is used in this product?

A: Depending on your model the diskG uses either AES 128-bit or 256-bit algorithm.

Q: Why could I not change my User Password which has the same digits as my Admin Password?

A: You can change it only in the Admin Mode. In the User Mode, the User Password which has the same digits is created in the Admin Mode cannot be changed or deleted.

Q: Why could I not initialize, partition or format the diskG?

A: Ensure that you have administrator privileges. You can use only the administrator account to initialize, partition or format the diskG in the Admin Mode.

Q: Do I require "Admin Rights" for the diskG to work?

A: No, since the diskG does not require any software to be installed and the encryption/decryption is performed in Hardware on the drive itself, "Admin Rights" are not required.

Q: I'm getting a continuously flashing red light what is wrong?

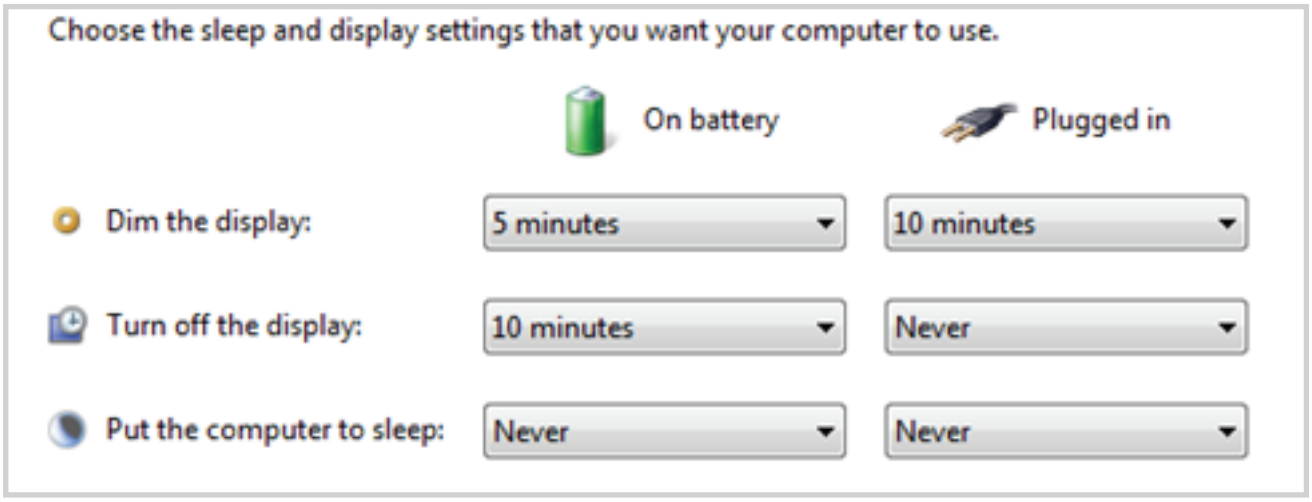
A: You have entered an incorrect PIN too many times and have triggered the brute force attack protection; you can reset this counter by referring to the `Brute Force Protection` section 15 of this manual. When trying again ensure you are using the correct PIN as too many lockouts are irreversible.

Q: My diskG locks for no reason when connected to my computer whilst I'm using it, what is causing this?

A: The issue you are having is being caused by power saving settings on your PC or Laptop so please see below and make the appropriate changes to your computer and this will stop the diskG from locking as when your computer is power saving it switches off data to the USB ports and our products see that as `Disconnect` and are designed to lock when this is detected.

Microsoft Windows

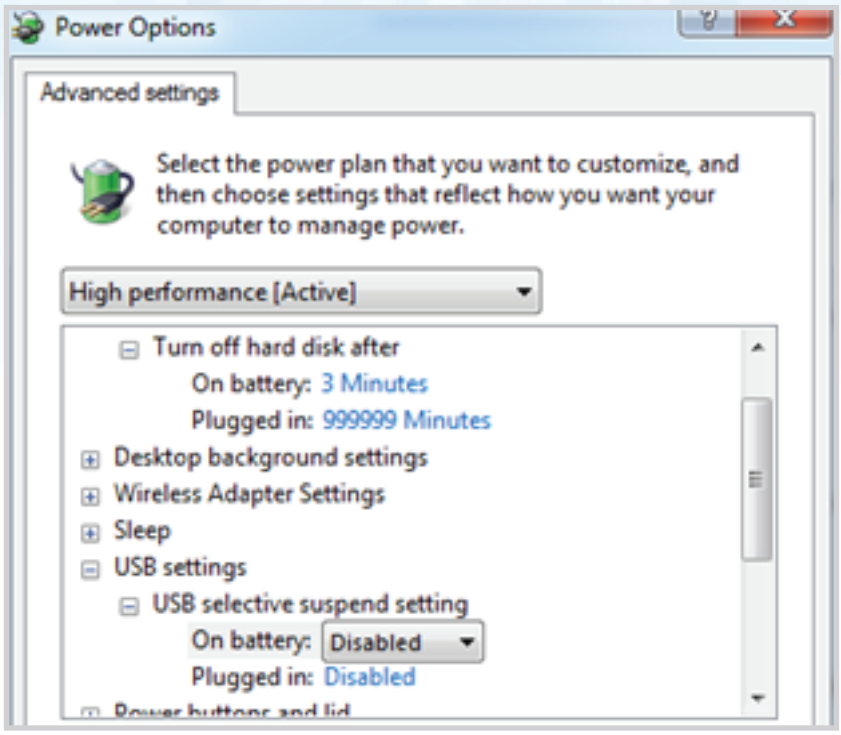
Doing the following will prevent Windows from switching off the diskG, go to **'Control Panel'** & **'Power Options'** , the easier option is to disable power saving which means stopping the computer from `Sleeping` see below;



In addition go into `Advanced Settings` in `Power Option` to disable the following:

- Ensure the computer is set to sleep: Never (as above)
- Turn off hard disk after: 999999 Minutes
- USB selective suspend setting: Disabled

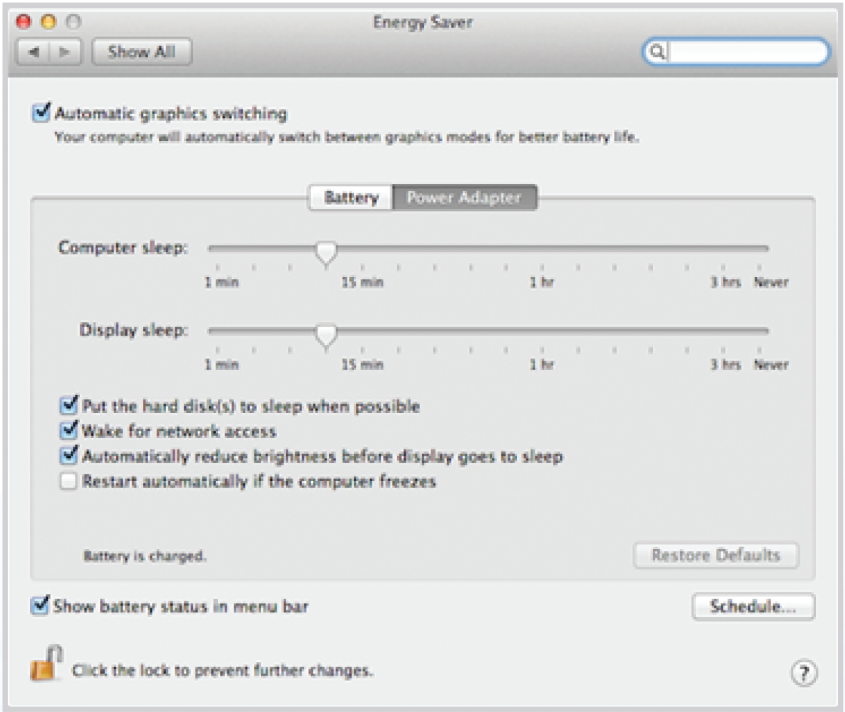
This will keep the diskG connected to the computer continuously on.


Power Options
Advanced settings
Select the power plan that you want to customize, and then choose settings that reflect how you want your computer to manage power.
High performance [Active]
Turn off hard disk after
On battery: 3 Minutes
Plugged in: 999999 Minutes
Desktop background settings
Wireless Adapter Settings
Sleep
USB settings
USB selective suspend setting
On battery: Disabled
Plugged in: Disabled

Apple Mac

The diskG keeps locking after 5-10 minutes on the Macs – This will be due the Mac's power saving as there is a setting to switch off hard drives that are idle after a fix period of time see below;

The settings in Energy Saver preferences affect what happens when your Mac is left unattended for a period of time that you specify. Disable `Put the hard disk(s) to sleep when possible` to prevent the diskG going to sleep and so not locking. You will also need to stop the computer from sleeping to prevent the diskG from locking.



Note For Windows 8.1 users; You will need to install a Windows update (KB2919355) as well as follow the steps on pages 18 &19. Please go to this link and choose Method 2; http://support.microsoft.com/kb/2919355. Once the download option appears select KB2919355 and then download and install.

Q: My diskG locks when my computer sleeps/hibernates how can I stop this?

A: The only way to prevent this is by changing the power settings (Windows computers) of the computer so that it only switches of the monitor on hibernation/sleep and keeps power to hard drives and USB. On Apple MAC computers going to the power settings in `System Preferences` and clicking the do not suspend USB will keep the drive alive even if the MAC goes into full hibernation.

Q: The diskG will not power on when connected to my computer?

A: This only happens when the computer the diskG is connected to cannot provide enough power from the USB port to power the drive. This issue only appears on much older computers and/or imbedded systems like USB enabled medical equipment. It can be resolved by either trying all the USB ports on the computer or system as some ports can have less power than others or failing that use the USB Y-Power cable supplied with the diskG to ensure the correct power.

Q: I want to use my diskG with different Operating Systems how can that be done?

A: To make the diskG universally compatible with all the most common Operating Systems and embedded systems like USB enabled medical equipment, requires the drive to be formatted using the FAT file system. This is done by using 'Disk Management' in Windows, 'Disk Utility' on MAC OS/x or MKFS in Linux.

Q: How many unique User ID's can I create?

A: The Administrator feature allows enrollment of up to ten (10) unique User ID's and one (1) Administrator. If a user forgets their PIN, the diskG can be unlocked using the Admin PIN.

20. Technical Support

iStorage provides the following helpful resources for you:

iStorage's Website
http://www.istorage-uk.com

E-mail correspondence
support@istorage-uk.com

Telephone support with our Technical Support Department on **+44 (0) 20 8991-6260**.
iStorage's Technical Support Specialists are available from 9:00 a.m. to 5:30 p.m.
GMT - Monday through Friday.

21. Warranty and RMA information

Two Year Warranty:

iStorage offers a 2-year warranty on the iStorage diskG against defects in materials and workmanship under normal use. The warranty period is effective from the date of purchase either directly from iStorage or an authorised reseller.

Disclaimer and terms of warranty:

THE WARRANTY BECOMES EFFECTIVE ON THE DATE OF PURCHASE AND MUST BE VERIFIED WITH YOUR SALES RECEIPT OR INVOICE DISPLAYING THE DATE OF PRODUCT PURCHASE.
ISTORAGE WILL, AT NO ADDITIONAL CHARGE, REPAIR OR REPLACE DEFECTIVE PARTS WITH NEW PARTS OR SERVICEABLE USED PARTS THAT ARE EQUIVALENT TO NEW IN PERFORMANCE. ALL EXCHANGED PARTS AND PRODUCTS REPLACED UNDER THIS WARRANTY WILL BECOME THE PROPERTY OF ISTORAGE.
THIS WARRANTY DOES NOT EXTEND TO ANY PRODUCT NOT PURCHASED DIRECTLY FROM ISTORAGE OR AN AUTHORIzED RESELLER OR TO ANY PRODUCT THAT HAS BEEN DAMAGED OR RENDERED DEFECTIVE: 1. AS A RESULT OF ACCIDENT, MISUSE, NEGLECT, ABUSE OR FAILURE AND/OR INABILITY TO FOLLOW THE WRITTEN INSTRUCTIONS PROVIDED IN THIS INSTRUCTION GUIDE: 2. BY THE USE OF PARTS NOT MANUFACTURED OR SOLD BY ISTORAGE; 3. BY MODIFICATION OF THE PRODUCT; OR 4. AS A RESULT OF SERVICE, ALTERNATION OR REPAIR BY ANYONE OTHER THAN ISTORAGE AND SHALL BE VOID. THIS WARRANTY DOES NOT COVER NORMAL WEAR AND TEAR.
NO OTHER WARRANTY, EITHER EXPRESS OR IMPLIED, INCLUDING ANY WARRANTY OR MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, HAS BEEN OR WILL BE MADE BY OR ON BEHALF OF ISTORAGE OR BY OPERATION OF LAW WITH RESPECT TO THE PRODUCT OR ITS INSTALLATION, USE, OPERATION, REPLACEMENT OR REPAIR.
ISTORAGE SHALL NOT BE LIABLE BY VIRTUE OF THIS WARRANTY, OR OTHERWISE, FOR ANY INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGE INCLUDING ANY LOSS OF DATA RESULTING FROM THE USE OR OPERATION OF THE PRODUCT, WHETHER OR NOT ISTORAGE WAS APPRISED OF THE POSSIBILITY OF SUCH DAMAGES.

© iStorage, 2009. All rights reserved.
iStorage Limited, iStorage House, 13 Alperton Lane
Perivale, Middlesex. UB6 8DH, England
Tel: +44 (0) 20 8991 6260 | Fax: +44 (0) 20 8991 6277
e-mail: info@istorage-uk.com | web: www.istorage-uk.com